Detecting and Isolating Distributed Denial of Service Attack in Smart Grid Systems

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Karthikeyan B

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela, Odisha, 769 008, India

May 2014

Detecting and Isolating Distributed Denial Of Service Attack in Smarat Grid Systems

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

(Specialization: Information Security)

by

Karthikeyan B

(Roll No- 212CS2103)

under the supervision of

Dr. Bibhudatta Sahoo

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela, Odisha, 769 008, India

May 2014

Department of Computer Science and Engineering

National Institute of Technology, Rourkela

Rourkela-769 008, Odisha, India.

Certificate

This is to affirm that the work in the thesis entitled ***Detecting and Isolating Distributed Denial of Service Attack in Smart Grid Systems*** by ***Karthikeyan B*** is a record of an original research work carried out by him under my supervision and guidance in partial fulfilment of the requirements for the award of the degree of Master of Technology with the specialization of Computer Science in the department of Computer Science and Engineering, National Institute of Technology Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Place: NIT Rourkela
Date:

Dr. Bibhudatta Sahoo
CSE Department
NIT Rourkela, Odisha

Acknowledgment

I am thankful to various nearby and worldwide associates who have helped towards molding this thesis. At the beginning, I might want to express my true thanks to Dr. Bibhudatta Sahoo for his recommendation throughout my thesis work. As my supervisor, he has always swayed me to stay concentrated on accomplishing my objective. His perceptions and remarks helped me to build the general bearing of the research and to push ahead with research in profundity. He has helped me significantly and been a source of information.

I am really obligated to Dr. S.K Rath, Head-CSE, for his continuous encouragement and support. He is always ready to help with a smile. I am also thankful to all the professors of the department for their support.

My true thanks to my all friends and to everyone who has provided me with kind words, a welcome ear, new plans, valuable feedback, or their invaluable time, I am truly indebted.

Last, but not the least, I would like to dedicate this thesis to my family, for their love, patience, and understanding.

Karthikeyan B

Abstract

Smart grid(SG), which is considered as next generation power grid is an two way connected power system framework which enables easy monitoring and maintenance of power systems when compared to the existing power systems. Smart grid is also called as electrical grid or intelligent grid is an enhancement of 20th century power grid. Smart grid technically depends upon the network protocol and the topology over which it is constructed. Hence like the conventional connected systems, smart grid is also prone to number of security threats like Eavesdropping attack, data alteration attack, identity spoofing attack, compromised key attack, replay attack and distributed denial of service (DDOS) attack. In-spite of providing good technology to all the connected systems, there are frequent security breaches like DDOS attack which will extremely influence the availability of smart grid framework. Attacks targeting the availability like DDOS attack are the interruption of access or use of information which may further disrupt the power delivery. This thesis discusses detection and isolation of DDOS attack on Smart Grid. We have proposed three techniques to protect the framework against DDOS attack utilizing Marking system, TTL Value investigation and MAC value examination. The analysis of marking scheme has been carried out on *Network Simulator Version 2*. The identification of fake packets has been carried out using TTL value with help of *Cisco packet tracer, cola soft packet builder and Snort Intrusion detection tool*. The uniqueness of the MAC address and IP address are matched with the help of *Arpwatch* tool and *Snort Intrusion detection* tool to detect the fake MAC and IP address pair. With these schemes it is possible to pro-actively prevent the DDOS attack.

Contents

List of Figures

List of Tables

List of Abbreviations

SG	Smart Grid
DDOS	Distributed Denial Of Service Attack
MAC	Media Access Control Address
IP	Intrenet Protocol Address
ARP	Address Resolution Protocol
TTL	Time To Live
FTP	File Transfer Protocol
UDP	User Datagram Protocol
VBR	Variable Bit Rate
NS2	Network Simulator Version 2.0
ICMP	Internet Control Message Protocol
QOS	Quality Of Service
NIST	National Institute of Standards and Technology

Chapter 1

Introduction

Smart grid systems

Literature review

Motivation

Problem statement

Research contribution

Thesis organization

Chapter 1

Introduction

1.1 Smart grid systems

Smart grid is a new method of interconnected system for conveying power from producers to consumers in efficient, flexible and in more robust manner with high power-flow control, self-healing and with high data security using the digital technology [1]. According to the IEEE standard, Smart Grid is a mixture of power, communications and information technology for well advanced electric power system serving the power load. The word "Smart" in Smart Grid is included due to the added benefit of communication and intelligence to the existing power grid which eases the monitoring and maintenance of system. The merit of converting the conventional Power Grid systems to Smart Grid is; more efficient transfer of electricity, quicker restoration of power outages, reduced maintenance and operation cost, increased integration of large scale power source and security control. Smart Grid systems can make an automatic diversion of the power based on the needs and in the case of outages. It also helps to make energy efficient process by creating awareness among customers about the power usage. Significant research has to be done towards stabilizing Smart Grid for the purpose of changing the power grid into an efficient and intelligent electric power distribution system adaptable to the present environment.

The benefits of having a Smart Grid rather than having a general Power Grid Systems make a wide difference to both the users and for the organizers of power systems by providing intelligence to the system and reliability to the customers.

Some other the benefits of having Smart Grid systems are pointed out here [2]:

- Providing new services to the customers at the ease of a click
- Improving the resilience of the system against the outage
- Strengthening the system against security attacks
- Automation of routine maintenance work
- Efficient routing of power
- Enhancing the efficiency of existing system
- Access to historical data [3]
- Reduction of energy loss.

In Figure 1.1 given below gives a brief overview about the components of typical Smart Grid systems. According to IEEE smart grid, the entire smart grid system is divided into seven components namely: Bulk generator, Transmission, Distribution, Customer, Service Provider, Operations and Markets. Bulk generation indicates the procedure of handling and gathering power from renewable and non renewable energy source in huge quantity. Distribution domain delivers the electricity to and from the customers in smart grid. The distribution network connects the savvy meters and all intelligent field devices for managing and controlling them by means of two-way channel. The operations entity of the smart grid model manages and controls the electricity flow of all other domains inside the smart grid system. It uses two way communication channel between customers and substations. The Market domain, works and organizes all the members inside the shrewd lattice to give administrations like business administration, wholesaling, retailing and exchanging of vitality administrations. The Service Provider domain handles all outsider-operations among these domains. This incorporate web entrances that give vitality productivity administrations to clients, information exchange between the client and the utilities in regards to vitality administration and power supplied to homes and structures.

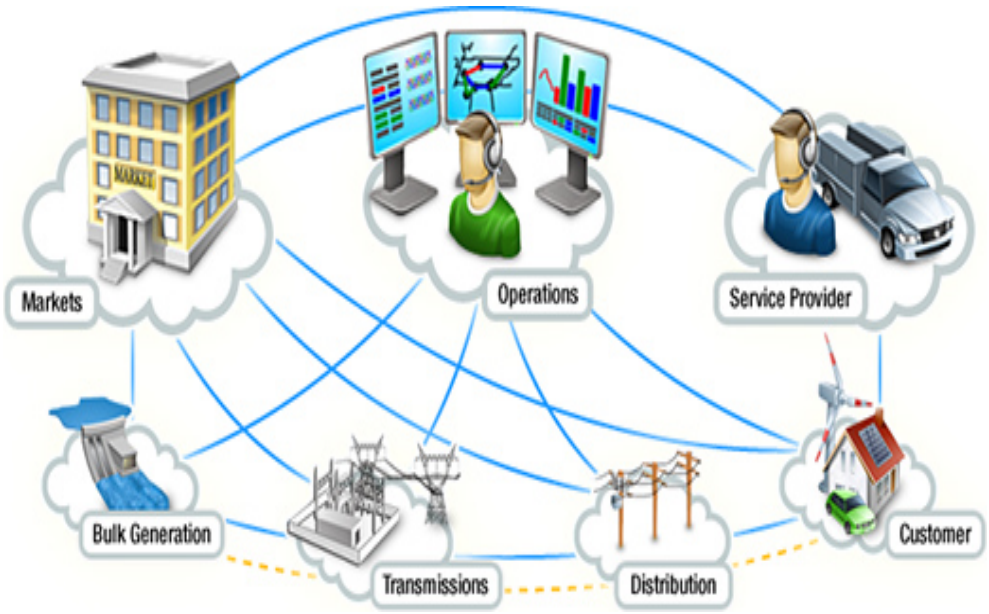

Figure 1.1: Conceptual smart grid model

Few issues exists in the Smart Grid Systems even though it has plenty of benefits over the traditional Power grid systems. Cyber security is an important area in the Smart Grid that has to be taken care. The incident of security breaches which raised the concern of users connected over the internet in past few years include Distributed Denial of Service Attack whose main goal is to bring the availability of resource to legitimate users by overloading it with traffic from multiple sources. They target a wide variety of resources, from banks to news websites and present a major threat to make sure people can publish and access important information over the grid. In Distributed Denial of Service attack, the attacker either takes control of multiple or single vulnerable system to create a spoofed IP address attack. The attackers in DDOS attack usually changes the source IP address to hide their identity which is called as spoofed IP address attack.

1.2 Literature review

Smart Grid systems have the goal to enhance performance of the existing power system by providing high availability, enhanced security, authenticated access control, easy maintenance and reduced cost[3] . To ensure the availability of critical real time power system, we must defend the system against all kind of security

attacks. Security threats over the Smart Grid systems are applicable to all the industrial systems[5]. Some of such threats are

- Denial of Service attacks [4],
- Eavesdropping [5],
- Man-in-the-middle attack [6],
- Identify Spoofing [6],
- Intrusion attack [6],
- Compromised key attack [4]

The Cyber security working group in the NIST Smart Grid panel has issued various guidelines for Smart Grid Cyber security to improve the performance over the above security issues [7]. Further three level security objectives are classified for Smart Grid based upon Availability, Integrity and Confidentiality.

- *Attacks targeting Availability* - The most important objective of Smart Grid system is to ensure reliable and timely access to the end user information. Attacks like DOS and DDOS can disrupt the availability of system for critical real time application.
- *Attacks targeting integrity* - Protecting against incorrect modification or removal of user data are more essential for the marketing purpose. Loss of integrity in smart grid systems leads to incorrect decision regarding the user billing data.
- *Attacks targeting confidentiality* - Preventing unauthorized access to data for preserving privacy is also a major objective of Smart Grid system. This is particularly necessary when private data should not be disclosed publicly.

Here we concentrate on the attack targeting availability. i.e, Distributed Denial of Service attack. The act of making a system or network resource unavailable to its destined users is termed as Denial of Service attack whereas in Distributed Denial

of Service attack, multiple compromised systems were used to target single machine causing denial of service attack. In DDOS attack, the approaching activity overflowed from various source pointing at single exploited person is for the most part gigantic to control it by blocking single IP location and it is exceptionally troublesome to discover contrast between ordinary and assault movement when it is spread crosswise over numerous sources.

DDOS is one of the prime threats in the current Internet world because of its ability to create a enormous volume of unwanted traffic. The primary purpose of this attacks is to prevent access to a particular resource like a Web site [8]. The first reported Large-volume DDOS attack occurred in August, 1999, against the University of Minnesota [8]. This attack ceases down the victim's network for more than two days. In the year 2000, DDOS attack stopped many major commercial Web sites, including Yahoo and CNN, from performing their normal operations [8]. D. Moore et al. [8] used backscatter analysis on three weeks datasets to evaluate the number, duration and focus of DDOS attacks to characterize their behaviour. They found that more than 12,000 attacks had occurred. Recently during the year 2013, massive 300Gbps attack was thrown against Spamhaus' website. Thus the severity of DDOS attack is increasing over every year. Hence in order to devise a broad solution for DDoS, there is a need to study and analyse the impact of DDoS attack against connected systems like Smart Grid. Here we have compared five different research papers which have used TTL value analysis and marking scheme as given in the below Table 1.1

Table 1.1: Related work

Authors	MAC value analysis	TTL value analysis	Marking scheme
Yao chen [9]	✗	✗	✓
Ryo [10]	✗	✓	✗
Cheng Jin [11]	✗	✓	✗
Qiang [12]	✗	✗	✓
Yaar [13]	✗	✗	✓

1.3 Motivation

Smart Grid Systems are the combination of diverse legacy frameworks with new technologies and architectural changes. To help this, security for smart grid has to be strengthened towards the attack targeting the availability, integrity and confidentiality of usual connected systems. Attacks targeting the loss of availability is the interruption of access or use of information which may further disrupt the power delivery. Henceforth we are persuaded to work on the attacks focusing on the availability.

1.4 Problem statement

In our proposed work we pro-actively scan every incoming packets and mitigate the DDOS attack using the Time To Live (TTL) value [10] and Media access control address (MAC) value analysis. Further we associate multiple routers to produce an Marking on each incoming packet to the victim using Marking based Detection And Filtering (MDADF) mechanism [9].

1.5 Research contribution

DDOS attack will extremely influence the availability of Smart Grid framework and hence we need to safeguard the system against it in the best possible way. Jelena et al. [14] [15] have used percentage of failed transactions that do not follow quality of service thresholds as a metric to analyse DDOS impact. They define a threshold-based model for the relevant traffic measurements, which is application specific. When the measurement value exceeds its threshold then it indicates poor services quality. But since transaction time period depends on the volume of data

being transferred and network load, absolute threshold cannot be set as the sole parameter. Subsequently we proposed three technique to protect the framework against DDOS attack utilizing Marking system, TTL Value investigation and MAC value examination.

1.6 Thesis organization

The remaining section of the thesis is organized as follows chapter-2 summarizes the security objectives and different types of security threats on Smart Grid, chapter-3 summarizes the Distributed Denial of Service Attack on Smart Grid, chapter-4 provides details on how DDOS attack is detected and isolated , chapter-5 provides the Conclusion and Future work.

Chapter 2

Security issues in smart grid

Security objectives

Security threats over smart grid

Attacks over the smart grid framework

Summary

Chapter 2

Security issues in smart grid

The customary Power Grid segment has coordinated electrical power framework with communication system to structure a two way channel which is known as, Smart Grid. This coordination has made the correspondence quicker and adaptable as well as more obvious to general society system. The advancement over the Ubiquitous computing and communication technology have initiated the smarter, dynamic and more interactive smart grid system which raises the amount of personal information involved and used in smart grid systems. This automatically raises the growth of low cost communication network, distributed energy resource, distributed storage devices and digital meters. In-spite of bringing great performance merit to the power sector it also has great potential risk in protecting itself against the Cyber threats.

2.1 Security objectives

The reliability of a Smart Grid System is depended upon the control and communication systems over which it was developed. Smart Grid needs high powered network connectivity to support new features and better network performance is based upon its protocols which is open to the global community. The security objective of smart grid is quite different from the other connected systems. It is important to take care that, any security countermeasure implemented on Smart Grid system does not affect its basic performance. Here we discuss various security objectives of smart grid systems like privacy, availability, authentication, non-reputability, integrity, authorization and third party protection.

2.1.1 Privacy

The measure of personal data included and utilized within Smart Grid system has drastically expanded with the advancement of savvy network. Savvy meters and other gadgets used in smart grid may give access to the intimate details of the customers. Protection issues of Smart Grid framework bargain with the way obliged data is going to be gathered, utilized and revealed. Further it is also important to know how Smart Grid would gather information about the individuals like the energy fluctuation of individual customer is so unique that it may be possible to identify the power system based upon the usage data. Smart meters and roaming smart grid devices may expose the data about consumers activity which leads to private information such as how many people live in the home, their schedule of using the home appliance and even sleeping patterns could be revealed easily.

2.1.2 Availability

Internet has made a large portion of the exercises on-line and this should continue expanding through the years. Consequently any attack focusing on its accessibility will simply disintegrate the human movement. Smart Grid frameworks must guarantee that unapproved individual or framework can get access or use to authorized components. Availability of smart grid must be considered with top care since power system play a vital role in our everyday life activity. Any malicious activity targeting the availability can be taken as denial of service attack which is motivated to slab the information over the network.

The services of many application are seriously harmed and thus part of business lose are caused because of these attacks. In DDOS situation, the attack originates from distinctive source and thus its all the more destroying. Subsequently there is a more terrific need to assess the brunt of attacks over Smart Grid.

2.1.3 Integrity

Integrity has to be maintained on every system to ensure that data is not modified by authorized or unauthorized person in the network. In Smart Grid system this

applies to maintaining the sensor values, product varieties and billing details. A attack targeting integrity in smart grid system usually corrupt either customer information or network information like usage, metering data, voltage readings or device status. The risk of attack focusing on data integrity in the power networks is very solid which includes false data injection attack by injecting the fake data into the system for attackers benefit.

2.1.4 Authentication

Authentication involves identifying the right person to enter the smart grid system and thereby preventing any malicious activity. Main concern of authentication involves identifying legitimate and illegitimate users using authentication standards.

2.1.5 Authorization

Authorization is the act of providing access control to the users who are eligible to do specific changes over the system. On a broader view, authorization differentiates between legitimate and illegitimate users for any system.

2.1.6 Nonrepudation and Third party protection

Nonrepudation refers to providing assurance that someone cannot deny over something. Nonrepudation refers to the ability to ensure that everyone cooperate in the system by the help of third party protection. Digital signature is used to ensure the data or document is mutually agreed and verified. In smart grid, nonrepudation is most needed to regulate the users with common agreement.

2.2 Security threats in smart grid

Security threats in Smart Grid systems are classified based upon the selfish users and malicious users. Selfish clients are those who are trying to get more network resources than it was allotted to them by tampering standards. Malicious users are the one who have no motto to get advantage for their benefit but still they aim to illegally fetch, update or delete information in the network. In smart grid malicious clients have to be taken care more seriously than selfish users since a lot of frameworks are utilized for observing and control reason apart from giving information help. Further selfish users are of less importance since amount of data transmitted over the network is very less which is usually the billing data.

Due to the modernization of the smart grid, security threats associated with other similar network are also applicable to the present smart grid system. Here we elaborate various such issues.

2.2.1 Eavesdropping

In Eavesdropping attack, the information packets are watched and once the attacker has the right to gain entrance to metering gadget of keen network, he is equipped for sniffing the whole information over the system. Listening in are by and large utilized for the business reason by checking and using the behavioural example of clients.

2.2.2 Data alteration

When the attacker has gained control over the grid, he can change the sniffed data as needed and send back the new version of data to the smart grid systems. Both the attackers and end users were also interested in modifying the usage for their own benefit.

2.2.3 Identity spoofing attack

In Smart Grid system each metering interface is assigned an unique IP address which is used reveal their identity. Once the attacker gains information about the system by eavesdropping, they can select any IP address from the network by

IP spoofing and can send false information. Identity spoofing is used by DDOS attack when flooding data packets. Man-in-the-middle, message replays, network spoofing attack are some of the common identity spoofing attack [6].

2.2.4 Compromised key attack

Compromised key attack are often possible in metering network of smart grid where the system uses identical key for encryption and decryption of the metering data. If the key which is being used to encipher the information is compromised then it is very easy to calculate the decryption key thereby gaining access to metering data which is modified by consumer to send false metering data. Utility operator gains access to the metering infrastructure to the utility plan of consumers.

2.2.5 Replay attack

Replay attacks can be launched when an attacker gain access to smart meters and inject control signals to the system. The attacker first needs to record data transmitted from customer to smart meters and analyse them to achieve customers characteristics of power usage. After analysing, the attacker may inject the data to grid system. Two common purpose of this attack is to steal energy and other is to cause physical damage to the system [16].

2.3 Attacks over the smart grid framework

Smart Grid framework is divided into four components and classified based upon the common attack possible as: power generator, service provider, Smart Grid system and customer. Power generator is responsible for generation and distribution of power to the service provider. Service provider does the monitoring operation over the entire framework for the purpose of billing and routing. Smart Grid system component does the job of load balancing, encrypting and decrypting of user billing data between each customer. Further it takes care of authentication and authorization over the framework. The encrypted data which is received from different customers are decrypted and sent back to the service provider. Different

types of attack that are commonly found over the above said smart grid systems framework are Eavesdropping, Denial of Service attack, Data alteration, Identity Spoofing, Compromised Key attack and Replay attack. Framework depicting the possible attack over different components of Smart Grid network is shown below in the Figure 2.1

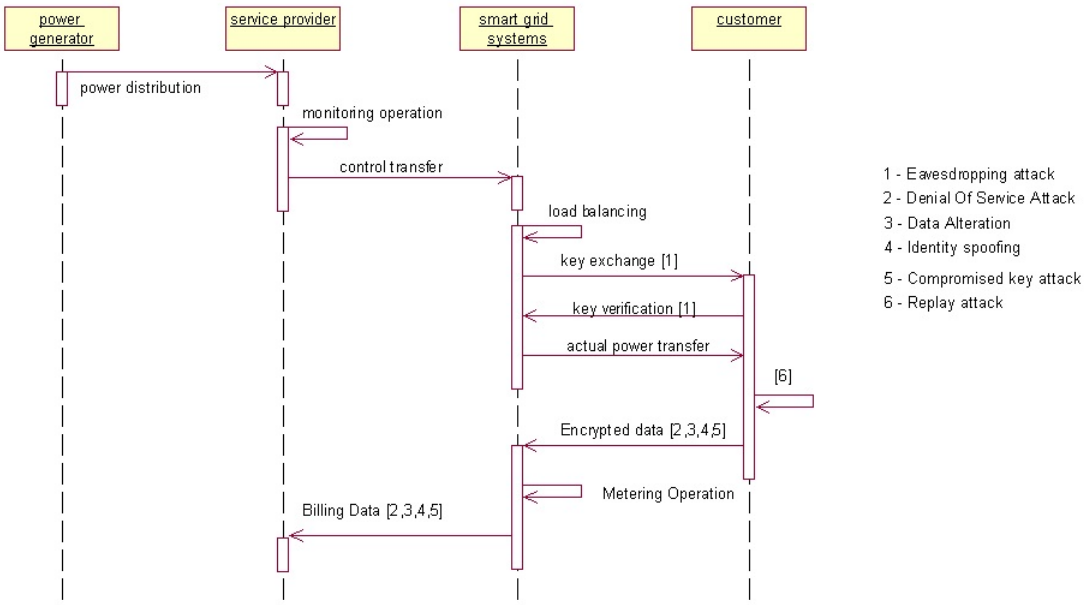

Figure 2.1: Attacks on smart grid framework

2.4 Summary

In this chapter, we have seen the basic security objectives and different security threats over the Smart Grid system. Further, sequence of attack possible over the Smart Grid Framework is explained to have a brief idea on the real time attack scenario over the system.

Chapter 3

Distributed Denial of Service Attack on Smart Grid Systems

Chapter 3

Distributed denial of service attack on Smart Grid

Primary goal of Smart Grid System is availability. Denial of Service attack can severely impact the availability of smart grid system by degrading the communication performance. As the global network increases in size, the attack volume also increases giving birth to the raise of Distributed Denial of Service Attack.

Internet was assembled without much stress about the security and thus pernicious clients misuse each part of it. The incident which has triggered the interest of many engineers in past few decades is the DDOS attack whose whole purpose is to cut down the availability of services provided over the network to its authentic clients. This is carried out by discovering vulnerabilities in applications, protocols or by depleting the network and computational asset or memory of victimized person. In Distributed Denial of Service, the attacker first takes control of huge number of systems which are traditionally called zombies and then utilize them to send large volume of packets in parallel which are valid most of the time. The attackers in DDOS attack usually modify their identities to hide their presence and make it difficult to differentiate between legitimate and illegitimate traffic packets. This idea of changing the identity with the help of IP address is called as IP Address spoofing.

3.1 Classification

Attacks based on communication

Based upon the communication between attacker and the victim, we can define two type of DDOS attack:

- Attack with Direct Communication
- Attack with In-Direct Communication

In *Attack with Direct Communication*, both attacker and victim need to have gained knowledge of each other identity to communicate. Main drawback of this approach is that compromising one machine can lead to the finding whole network responsible behind the attack.

In *Attack with In-Direct Communication*, the identity of attacker is not known to victim. The attacker initiates the attack with the help of multiple zombies present between victim and attacker. Most of the time, the attack created by zombies are not known to themselves.

Classification by degree of automation

During the attack , the attacker has to find the suitable zombies and contaminate them to create DDOS strike. Based on the level of mechanizing the attack has carried, Jameel Hashmi.et.al [17] classified the DDOS attack into three types:

- Manual Attack
- Semi Automatic Attack
- Automatic attack

In *Manual Attack*, the attacker manually scan the remote machine for its vulnerabilities to broke them and install the strike code. In *Semi Automatic Attack*, the attacker utilizes the computerized projects as a part of zombies for checking and bargaining the victimized person machine. In *Automatic attack*, the need for communication between attacker and zombies are avoided. Both semi-automatic and automatic attacks use compromised systems by sending programmed filtering and spread methods.

Classification based on random scanning

During the phase of randomly scanning for the victim, each compromised host probes the victim machine with different seed. This obviously creates huge volume of traffic. Attacks are classified based upon the scanning of victim into four types:

- Attacks based on Hit-list Scanning
- Attacks based on Topological Scanning
- Attacks based on Permutation Scanning
- Attacks based on Local Subnet Scanning
- Attacks based on Central Source Propagation
- Attacks based on Back Chaining Propagation

In *Hit-ist Scanning*, attacker probes for all the address given in the externally supplied list. When it finds the unstable machine, it sends one half of the initial hit-list to other recipients and keeps the remaining half.

In *Topological Scanning*, attacker uses the data on victim to select new victims. Email based attacks are based upon the topological scanning.

In *Permutation Scanning*,all the traded off machines impart a typical IP location space where every IP location is mapped to a list in this schedule. The machine starts checking by utilizing the file registered from its IP address as an introductory point. At whatever point it sees an effectively traded off machine, it chooses another arbitrary starting.

In *local subnet scanning*, attacker scans for the targets that are available within the subnet of available victim.

In *Central Source Propagation*, the attacker after compromising the agent machine downloads the attack script from the central source and operate on it.

In *Back-Chaining Propagation*, attack code was downloaded from the system that was already compromised and use it to exploit other system. Back chaining propagation avoids single point of failure.

3.2 DDOS defence mechanism

DDOS defence mechanism is classified into three categories [9] as given below

- Preventive Defence Mechanism
- Source Tracking Mechanism
- Reactive Solutions Mechanism

3.2.1 Preventive defence mechanism

Preventive Defence Mechanism points at enhancing the resistance level of framework via completing preventive measures even before the victimized person was affected. *Proactive server roaming scheme* [18] follows preventive defence mechanism where the system has several number of distributed servers and the area of server changes among them using secure roaming algorithm. Only the legitimate users will know the servers roaming time and address of new available server. All accessible connections are dropped when the server begins wandering, so that just the substantial clients can get benefits at the outset of each one meandering session before the attacker finds the dynamic server once more.

3.2.2 Source tracking

Source tracking method tries to trace down the source of attacks so that the attacker can be eliminated from the network. The existing solution falls under four groups [9]:

- Packet Marking
- Message Trace-back
- Logging
- Traffic observation

In *Packet marking Scheme*, path information of packets are encoded inside each packets as they are travelling through web. This idea is first implemented

by Savage et al. [23] called as probabilistic packet marking (PPM) plot in which switches include way data into the distinguishing proof field of IP header in every packet with certain likelihood so the end client can remake the attack path utilizing the markings and accordingly follow out the wellspring of attack. Path Identifier mechanism proposed by Abraham Yaar et al. [19] follows marking scheme in which way unique mark is inserted in every packet, in this way empowering the victimized person to recognize packets crossing the same way through web paying little respect to IP location ridiculing. This permits the exploited person to take proactive measure against DDOS attack.

In *Message traceback scheme*, routers produces ICMP traceback messages for a percentage of the approaching information and send it with them. We can find the creativity of packets by preparing their TTL refinement. A few elements to be acknowledged for assessing the worth of ICMP messages are the separation of terminus from the switch, how rapidly the packets are accepted after the begin of attack and whether the ends of the line wishes to get it or not.

In *Logging scheme*, data about packets are logged at routers. The route to the attacker could be perceived by the router exchanging data with each other.

In *Traffic-observation Scheme*, attack way is dictated by watching the rate of progress of movement on victimized person. Throughout attack stage, assaulter send tremendous number of packets to the victimized person. Via completing the connection test constantly, the attacker might be discovered.

3.2.3 Reactive solutions

In reactive measures for DDOS protection,advancing attack is gotten and structure reacts to it by controlling the stream of strike packets to diminish the impacts of attack. Path Identifier scheme proposed by Yaar et al. [9] utilizes the thought of packet stamping by filtering the attack packets as opposed to attempting to discover the wellspring of attack packets.

3.3 Summary

In this chapter we have briefed about Distributed Denial of Service attack and its classification. Further, defence mechanism to handle DDOS attack was also analysed.

Chapter 4

Prevention and Isolation Methodology

General flow structure

Marking scheme

Simulation methodology

Simulation parameter

TTL value analysis

MAC value analysis

Summary

Chapter 4

Prevention and Isolation Methodology

4.1 General flow structure

We use three methods to detect and isolate DDOS attack. The three methods are Marking Scheme, TTL Value analysis and MAC value analysis. If the packets which are found positive in any of the methods then it has to be reject to enter the victim system. Here MAC value analysis works only when the attack packets are originated within the network. Similarly TTL value analysis works only when the packets are originated outside the network since packets which are originated within the network has no change in TTL Value. Marking Scheme works out only when the routers coordinate with each other to eliminate the DDOS attack. Flowchart given in the below Figure 4.1 describes the overall process of our algorithm.

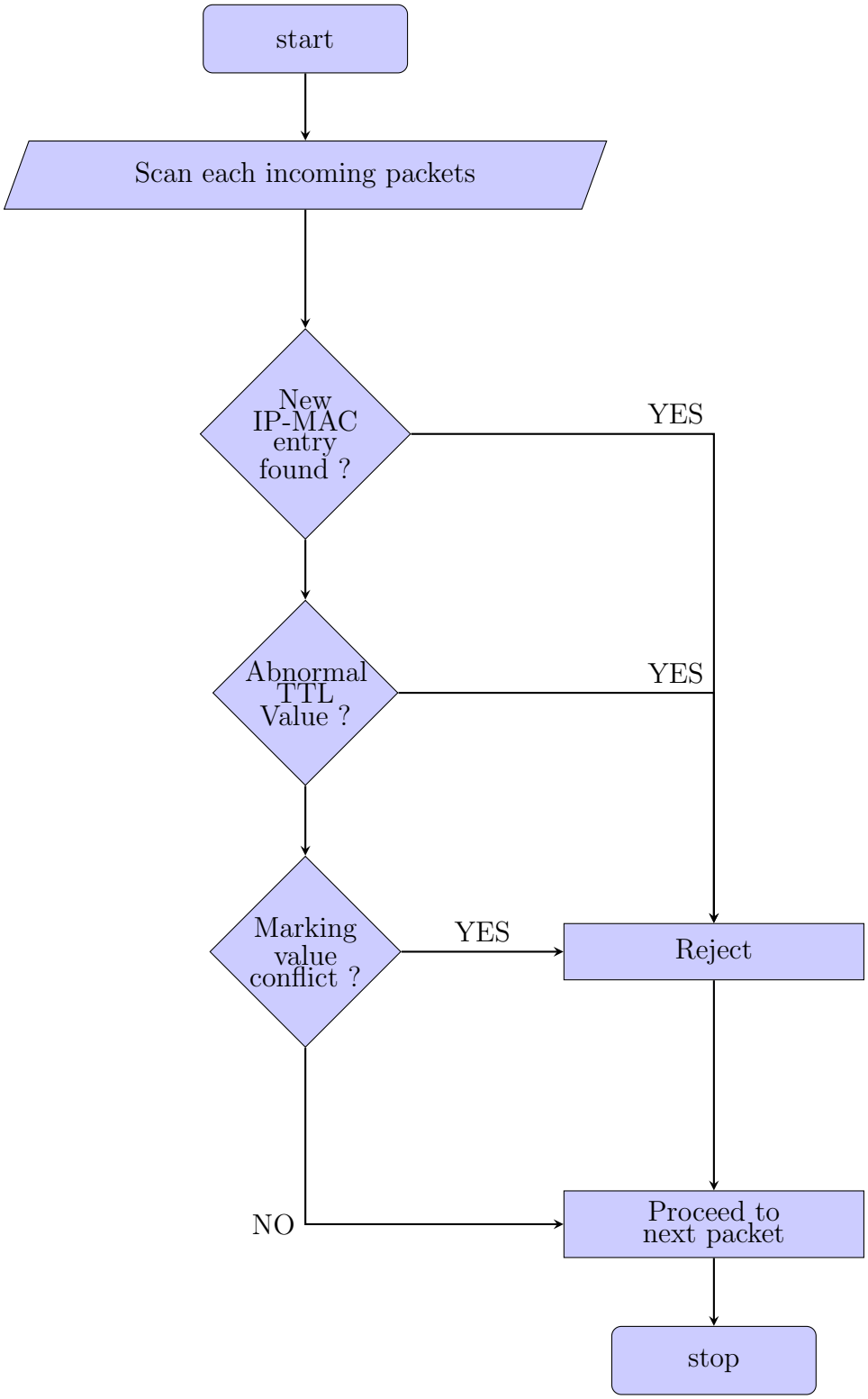

Figure 4.1: General flow structure

4.2 Marking scheme

Distributed Denial of Service attack is crumbling the internet every day. Traditional approach to protect the system against DDOS attack is to provide Source IP address of the attacker and path it travelled. With this information, the attacker can reach out the Internet Service Provider to drop all packets coming from the specific attacker. But it is very difficult to detect and stop the DDoS attacks, particularly those attack which uses IP address spoofing to disguise those attack flow. Though the source IP address is changed by the attackers, the path it has taken to reach the victim is totally determined by the network topology and routers present inside it. Unlike the other methods, Marking scheme can very well distinguish attack data from the normal data flow by the legitimate users. In marking scheme, each packet is embedded by certain marking, enabling the victim to identify the packets which are not from legitimate users by checking each packet regardless of IP address spoofing. Each packet travelling in the same path carries the same marking identification and hence the victim can pro-actively defend themselves against DDOS attack.

4.2.1 Simulation setup

The cost and effort of building a real time distributed network involving thousands of systems is very high and hence there is the need for constructing simulation system raises for the research work.

- We use the popular Network Simulator NS2 for simulating the network where multiple routers coordinate to produce an marking over each packet.

4.2.2 Simulation methodology

We have divided the work into three phase: Marking method, TTL Value analysis and MAC value analysis. Network simulator NS2 was used for packet marking analysis. Flow chart depicting the simulation methodology of marking scheme is given below in the Figure 4.2

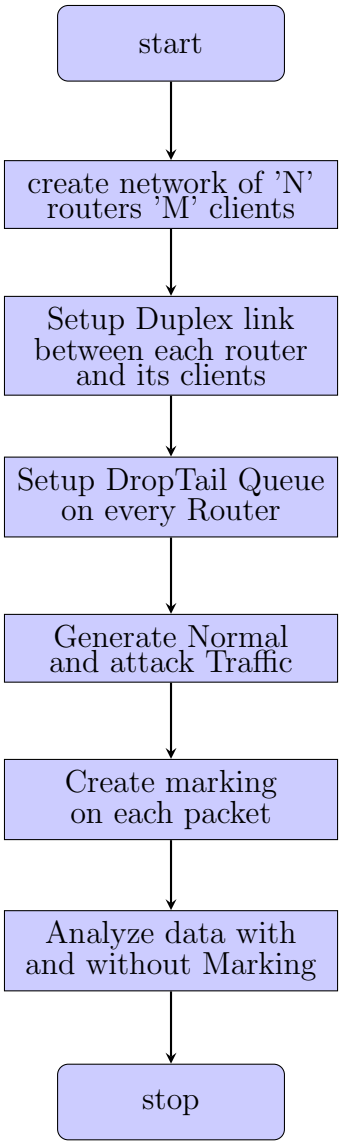

Figure 4.2: Marking scheme flowchart

In our proposed marking scheme, we create network topology consiting of 'N' routers with 'M' clients each where each client and its router are having duplex link connection. DropTail queue has setup on every router. In drop tail queue each packets are treated as same. In drop tail queue, when the queue limit has exceeded its maximum capacity then newly arriving packets are dropped until the queue is having enough buffer space to accept incoming packets. UDP and FTP traffic is generated over the network in Variable Bit Rate(VBR) flow. Mean bandwidth of FTP/UDP traffic, http to ftp ratio, total number of aborted downloads were calculated based on the traffic pattern.

4.2.3 Simulation parameter

We have taken the following parameters given in Table 4.1 for the Marking Scheme using network simulator NS2.

Table 4.1: Network simulation parameter

Simulation Parameter	**Description**
Number of Download	Total number of downloads in session
Request Interval	Time gap between each download request
Session Interval	Time gap between each session
Abort Time	Time taken for connection Abort
Active Interval	Time gap to check number of active download
Monitor Interval	Time gap to monitor buffer occupation
Bottleneck Bandwidth	Maximum limit for Queue
Tolerance Time	Time interval to check the number of failures
Connection Count	Number of FTP and UDP connection

4.2.4 Simulation result

In marking scheme, results are analysed based on two scenarios:

- Data packets are travelled directly between source and destination
- Data packets not travelling directly between source and destination.

When IP spoofed packets are used for DDOS attack, the path which each packet has taken will differ rather than original path destined for the particular IP address. Hence we use the deviation in the performance metrics over the change

in path to locate the occurrence of DDOS attack in network. Each connection is made up of 50 sessions with each session having 10000 download with bottle neck bandwidth of 1.5 Mega bits and request size of 5000 bits. Simulation of higher data flow is created with 50000 sessions with each session having 10 million downloads at the bottle neck bandwidth of 1.5Mb. Results derived from above specification are analysed to prove that data with peak curve is the sign of attack and hence the algorithm to isolate the attack packets has to be initiated. Average computation data for 10/50 clients without implementation marking is given below in the Figure 4.3 and Figure 4.4. Simulation results for 10 and 50 clients with normal and attack data flow with marking scheme implemented is shown in the Figure 4.5 and Figure 4.6

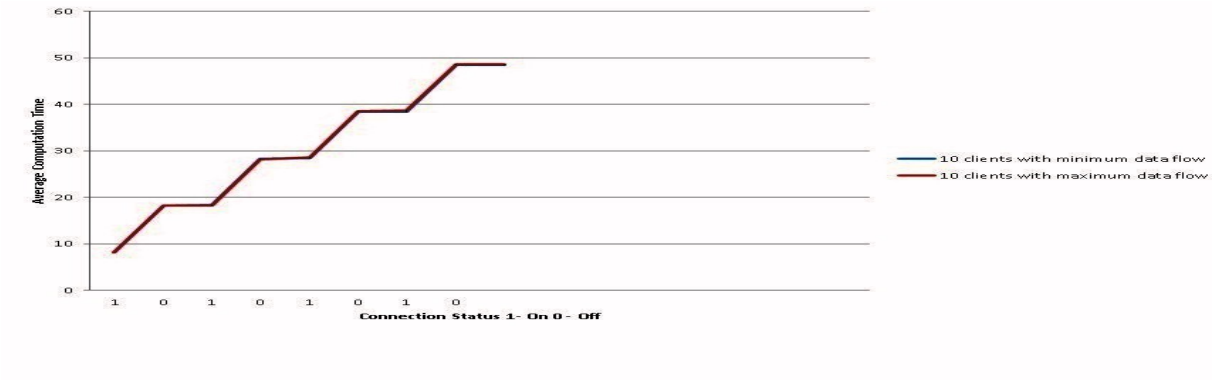

Figure 4.3: Average computation Data for 10 clients topology

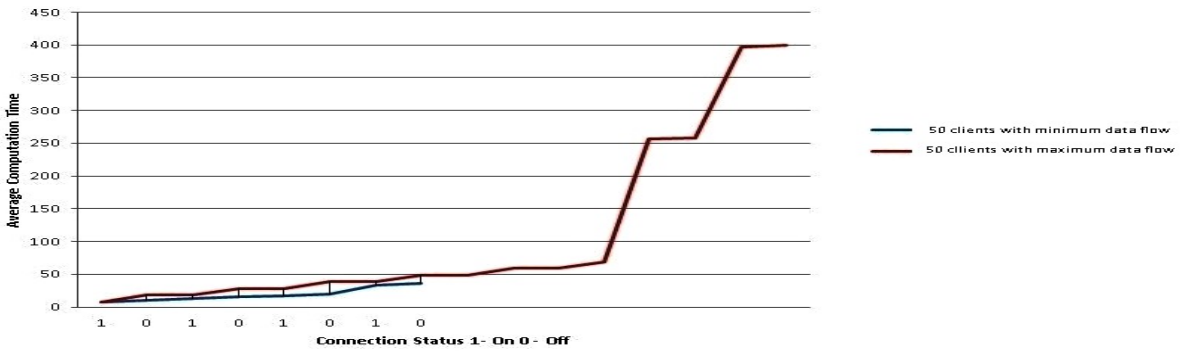

Figure 4.4: Average computation data for 50 clients topology

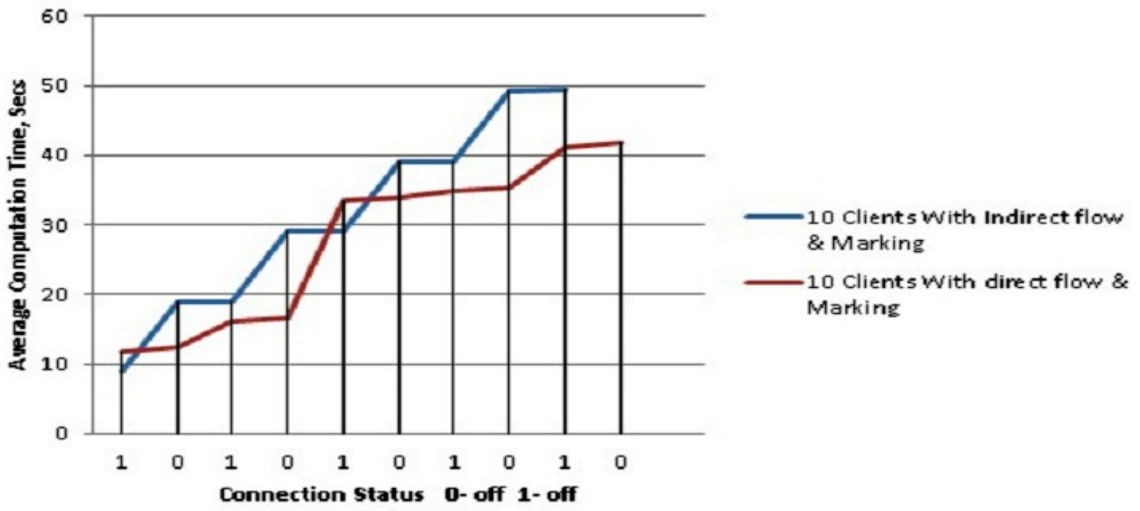

Figure 4.5: Comparison for 10 clients topology with marking

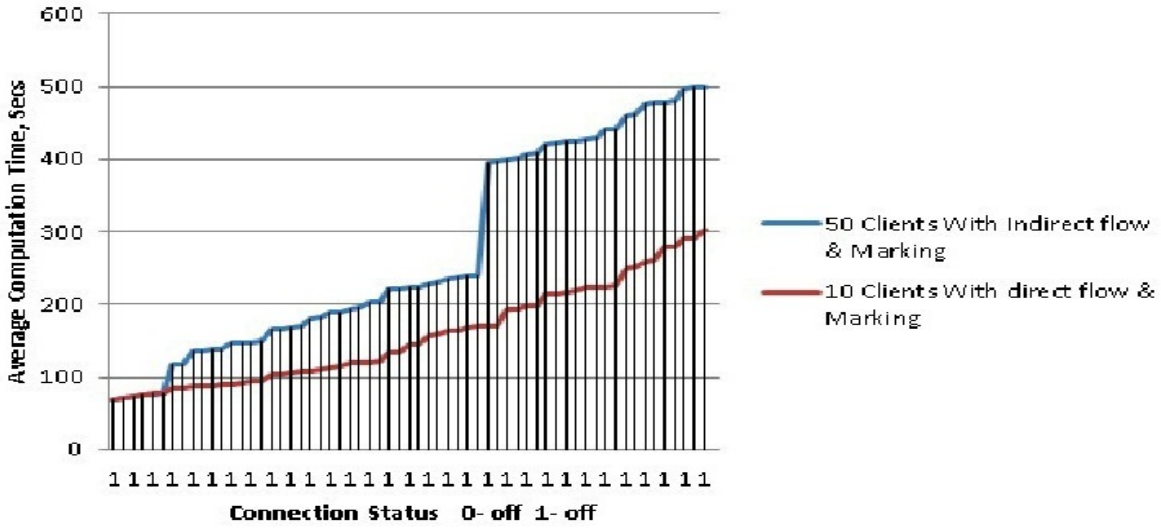

Figure 4.6: Comparison for 50 clients topology with marking

4.3 TTL value analysis

In Internet, every IP packet goes accross not more than 30 routers before reaching its destination. But some IP packets have abnormal TTL values which is decreased by more than 30 hops. We assume that IP packets with strange TTL values in IP headers as malicious packets and hence it is discarded. These packets are likely to be generated by special tools. Every computer fix the TTL value when it sends the packet based upon the operating system and the protocol which sends the packet. It is possible to estimate the total number of routers between source and destination using the TTL values. TTL Values of popular operating system were given below in the Table 4.2.

Table 4.2: TTL values of different operating systems

Operating system	**Protocol**	**TTL Value**
Linux kernel 2.2.14	ICMP	255
Windows Server 2008	ICMP, TCP, UDP	128
Windows 7	ICMP, TCP, UDP	128
Windows XP	ICMP, TCP, UDP	128
Free BSD 5	ICMP	64
MACOS 10.5.6	ICMP, TCP, UDP	64
Solaris 2.8	TCP	64
Sun OS 5.7	ICMP ,TCP	255

Tools used to implement TTL value analysis are,

- Cisco packet tracer, for simulating real time network depicting the smart grid
- Cola soft packet builder, to create a packet with fake TTL value
- Snort, an IDS tool to detect and isolate the packets with fake TTL value which falls in the range of abnormal TTL value

TTL values of normal and abnormal IP packets based upon the average hop count is given below:

Normal TTL value: if $30 < ttl <= 64 : 98 < ttl <= 128 : 225 < ttl <= 255$

Abnormal TTL value: if $1 < ttl <= 30 : 64 < ttl <= 98 : 128 < ttl <= 225S$

Cisco Packet tracer is used to simulate a network topology consisting of six clients connected to two server via three routers and two switch. Each node ping's the node present in other network to test the decremented TTL value. Below Figure 4.7 shows the Network created using Cisco packet tracer to analyse the TTL values.

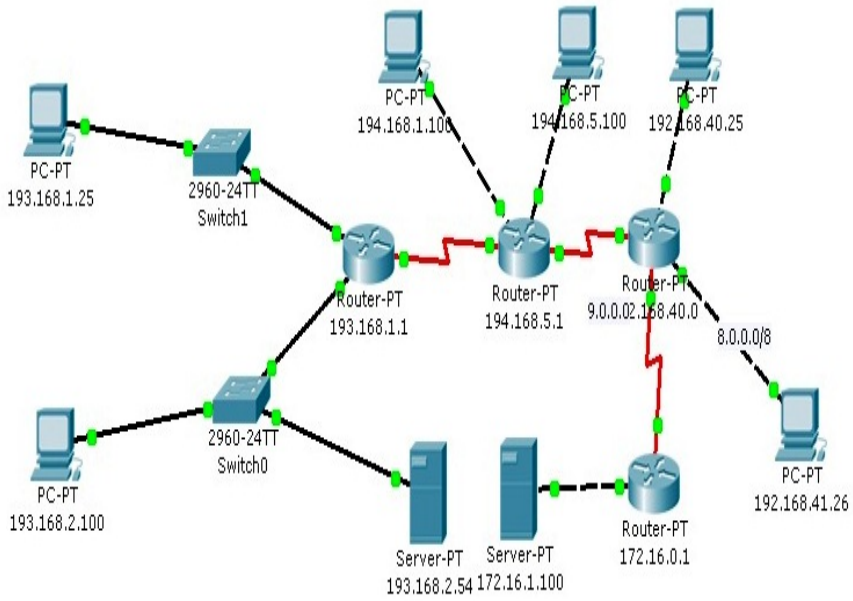

Figure 4.7: Network used for TTL value analysis

4.4 MAC value analysis

Many IP addresses attached to the same MAC would mean that many IP's coming through the same interface and hence those packets can be rejected with the help of table maintaining the list of source with its IP Address and MAC address. In most of the modern attacks, single attacker create random source flooding attack and hence it is easy to distinguish the source with fake MAC address. Hping3 tool is used to create Random source flooding attack which creates thousands of Packets in few minutes. It produces an real time DDOS attack with same MAC address. But MAC address does not appear in the IP packet once it crosses the network on which originates. Hence MAC value analysis is useful only when the fake IP packet raises within the network. ARPwatch tool is used to analyse the list of newly added IP and MAC pairs in the ARP table. ARPwatch tool produces an alert when there is an new entry of new IP address and MAC value pairs into the ARP table which can be verified with the help of Wireshark tool also. Figure 4.8 shows the result of arpwatch tool depicting the occurrence of changed MAC and IP pair.

Tools used: Hping, ARPWatch, Snort, Wireshark

- Hping tool is used to create an random source flooding attack
- ARPwatch is used to monitor the network for IP and MAC address information along with time-stamp
- Ethernet traffic activity like Changing IP and MAC address address is maintained in the database and dropped using Snort tool
- Wireshark is used to cross verify the presence of fake IP and MAC entry

```
From: root (Arpwatch)
To: root
Subject: new station

            hostname: <unknown>
          ip address: 192.168.40.77
    ethernet address: 0:23:4e:d9:17:1f
     ethernet vendor: Hon Hai Precision Ind. Co., Ltd.
           timestamp: Monday, May 5, 2014 11:28:29 +0530
arpwatch: bogon 192.168.41.242 e8:39:35:36:c7:60
arpwatch: bogon 192.168.41.249 78:ac:c0:97:35:9e
arpwatch: bogon 192.168.41.242 e8:39:35:36:c7:60
arpwatch: bogon 192.168.41.249 78:ac:c0:97:35:9e
arpwatch: bogon 192.168.41.242 e8:39:35:36:c7:60
arpwatch: bogon 192.168.41.249 78:ac:c0:97:35:9e

From: root (Arpwatch)
To: root
Subject: changed ethernet address

            hostname: <unknown>
          ip address: 192.168.40.27
    ethernet address: 0:f:fe:d9:a3:46
     ethernet vendor: G-PRO COMPUTER
old ethernet address: 0:1d:7d:5c:23:17
 old ethernet vendor: GIGA-BYTE TECHNOLOGY CO.,LTD.
           timestamp: Monday, May 5, 2014 11:28:32 +0530
  previous timestamp: Sunday, May 4, 2014 18:47:38 +0530
               delta: 16 hours
arpwatch: bogon 192.168.43.103 84:2b:2b:c0:3c:80
arpwatch: bogon 192.168.41.242 e8:39:35:36:c7:60
arpwatch: bogon 192.168.41.249 78:ac:c0:97:35:9e
```

Figure 4.8: MAC value analysis

4.5 Summary

In this chapter we presented various technique to prevent the Distributed Denial of Service attack in Smart Grid system. Simulation results has shown that marking scheme helps to easily differentiate the attack packets compared to the normal legitimate packets.

Chapter 5

Conclusions and Future Work

Chapter 5
Conclusions and Future work

This thesis deals with detection and isolation of DDOS attack in Smart Grid systems by using three methods. First method involves detecting fake packets which are created by the attacker during Distributed Denial of Service attack by comparing TTL value. But still there are packets which are escaping from this method since attacker now uses more sophisticated software's where they can change the TTL Values also. Hence we need a method which detects the packet escaped from the first method. So we created second scheme which uses marking scheme to produce an mark over each IP packet to find and isolate the attack packets. Each packet travelling across same router have similar kind of marking. Hence the fake packets which are having an Marking irrespective of its network can be detected. Marking scheme is useful when the routers among all network cooperate to find the attack path. There are cases where the DDOS attack were created within the network targeting another system inside the network. So we created third scheme which uses MAC value to differentiate fake packets Since two packets coming from two different users cannot have same MAC value.

In future we can extend the work done to prevent DDOS attack, when the attacker changes both the MAC and IP address. We can Integrate the TTL value analysis and Marking scheme together at Router level to detect and prevent DDOS attack.

Bibliography

[1] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. *Communications Surveys & Tutorials, IEEE*, 14(4):998–1010, 2012.

[2] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart gridthe new and improved power grid: a survey. *Communications Surveys & Tutorials, IEEE*, 14(4):944–980, 2012.

[3] Gianni Fenu, Marco Nitti, and Pier Luigi Pau. A complex network approach for a regional power grid analysis. In *Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on*, pages 45–50. IEEE, 2012.

[4] Mini S Thomas, Ikbal Ali, and Nitin Gupta. A secure way of exchanging the secret keys in advanced metering infrastructure. In *Power System Technology (POWERCON), 2012 IEEE International Conference on*, pages 1–7. IEEE, 2012.

[5] Jingcheng Gao, Yang Xiao, Jing Liu, Wei Liang, and CL Chen. A survey of communication/networking in smart grids. *Future Generation Computer Systems*, 28(2):391–404, 2012.

[6] T. Littler S. Sezer Eul Gyul Im Z.Q. Yao B Pranggono H F Wang Y. Yang, K. McLaughlin. Man-in-the-middle test bed investigating cyber-security vulnerabilities in smart grid in scada systems, sustaniable power generation and supply, 2012.

[7] Guidelines for smart grid cyber security NISTIR 7628 Cyber Security Working Group. The smart grid interoperability panel, 2010.

[8] Monika Sachdeva, Gurvinder Singh, Krishan Kumar, and Kuldip Singh. Measuring impact of ddos attacks on web services. 2010.

[9] Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El-Saddik, and Amiya Nayak. Detecting and preventing ip-spoofed distributed dos attacks. *IJ Network Security*, 7(1):69–80, 2008.

[10] Ryo Yamada and Shegeki Goto. Using abnormal ttl values to detect malicious ip packets. *Proceedings of the Asia-Pacific Advanced Network*, 34:27–34, 2013.

[11] Cheng Jin, Haining Wang, and Kang G Shin. Hop-count filtering: an effective defense against spoofed ddos traffic. In *Proceedings of the 10th ACM conference on Computer and communications security*, pages 30–41. ACM, 2003.

[12] Qiang Li, Hongzi Zhu, Meng Zhang, and Jiubin Ju. Simulating and improving probabilistic packet marking schemes using ns2. In *Parallel and Distributed Computing, Applications and Technologies, 2005. PDCAT 2005. Sixth International Conference on*, pages 348–352. IEEE, 2005.

[13] Abraham Yaar, Adrian Perrig, and Dawn Song. Pi: A path identification mechanism to defend against ddos attacks. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pages 93–107. IEEE, 2003.

[14] Jelena Mirkovic, Alefiya Hussain, Brett Wilson, Sonia Fahmy, Peter Reiher, Roshan Thomas, Wei-Min Yao, and Stephen Schwab. Towards user-centric metrics for denial-of-service measurement. In *Proceedings of the 2007 workshop on Experimental computer science*, page 8. ACM, 2007.

[15] Jelena Mirkovic, Sonia Fahmy, Peter Reiher, Roshan Thomas, Alefiya Hussain, Steven Schwab, Calvin Ko, and VA Centreville. Measuring impact of dos attacks. In *Proceedings of the DETER Community Workshop on Cyber Security Experimentation*, 2006.

[16] Jong-Ho Lee Thien-Toan Tran, Oh-Soon Shini. Detection of replay attacks in smart grid systems. *CHECK IN INTERNET*, 34:27–34, 2013.

[17] Mohd Jameel Hashmi, Manish Saxena, and Rajesh Saini. Classification of ddos attacks and their defense techniques using intrusion prevention system. *International Journal of Computer Science and Communication Networks*, 2(5), 2012.

[18] R. Melhem D.Mosse S.M. Khattab, C. Sangpachatanaruk and T. Znati. Proactive server roaming for mitigating denial-of-service attacks. pages 500–504. Elsevier, 2003.

[19] A. Yaar, A. Perrig, and D. Song. Pi: a path identification mechanism to defend against ddos attacks. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pages 93–107, May 2003.

[20] Rabab Hassan and Ghadir Radman. Survey on smart grid. In *IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the*, pages 210–213. IEEE, 2010.

[21] Dacfey Dzung, Martin Naedele, Thomas P Von Hoff, and Mario Crevatin. Security for industrial communication systems. *Proceedings of the IEEE*, 93(6):1152–1177, 2005.

[22] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. volume 57, pages 1344–1371. Elsevier, 2013.

[23] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. Practical network support for ip traceback. *ACM SIGCOMM Computer Communication Review*, 30(4):295–306, 2000.